AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A public key certificate issuing system comprising:

a certificate authority for issuing a public key certificate of an entity which uses said public key certificate; and

a registration authority for sending a public key certificate issuing request received from an entity under control to said certificate authority;

said certificate authority being constituted by a plurality of certificate authorities each executing a different signature algorithm, transferring a public key certificate between said plurality of certificate authorities in response to said public key certificate issuing request received from said registration authority, attaching a digital signature on message data constituting said public key certificate in accordance with said different signature algorithm at each certificate authority, and issuing a multi-signed public key certificate storing a plurality of signatures based on different signature algorithms,

wherein said multi-signed public key certificate includes at least a basic area and an extended area, the basic area storing information identifying a first different signature algorithm executed by a first of the plurality of certificate authorities, and the extended area storing information identifying a second different signature algorithm executed by a second of the plurality of certificate authorities, and

wherein first and second signatures are generated by respectively applying the first and second different signature algorithms to information in both the basic area and the extended area.

2. (Original) The public key certificate issuing system according to claim 1, wherein said plurality of certificate authorities include a Rivest-Shamir-Adleman certificate authority for executing signature generation processing based on a Rivest-Shamir-Adleman signature algorithm and an elliptic curve cryptography certificate authority for executing signature generation processing based on an elliptic curve cryptography algorithm, said signatures stored in said multi-signed public key certificate including a signature based on said Rivest-Shamir-Adleman signature algorithm and a signature based on said elliptic curve cryptography signature algorithm.

3. (Original) The public key certificate issuing system according to claim 1, wherein at least one of said plurality of certificate authorities has a configuration for executing processing of storing a generated signature and signature information including signature algorithm information associated with said generated signature into an extended area of said public key certificate.

4. (Previously Presented) The public key certificate issuing system according to claim 1, wherein at least one of said plurality of certificate authorities has a configuration for executing processing of storing a generated signature into an area other than the basic area and the extended area of said public key certificate and storing signature information including signature algorithm information associated with said generated signature into said extended area.

5. (Original) The public key certificate issuing system according to claim 1, wherein at least one of said plurality of certificate authorities has a configuration for executing processing of storing, into said public key certificate, flag information indicating whether at least two signatures are included in said public key certificate.

6. (Currently Amended) A public key certificate issuing method having a certificate authority for issuing a public key certificate of an entity which uses said public key certificate and a registration authority for sending a public key certificate issuing request received from an entity under control to said certificate authority to issue said public key certificate in response to said public key certificate issuing request from said registration authority, said certificate authority being constituted by a plurality of certificate authorities each executing a different signature algorithm, including the steps of:

~~storing basic data in a basic area of the public key certificate;~~

~~storing extended data in an extended area of the public key certificate;~~

~~generating a digital signature based on a first signature algorithm derived from the stored basic data and extended data;~~

transferring a public key certificate between said plurality of certificate authorities in response to said public key certificate issuing request received from said registration authority;

attaching ~~the~~ digital signatures on message data constituting said public key certificate in accordance with said different signature algorithm at each certificate authority; and

issuing a multi-signed public key certificate storing a plurality of signatures based on different signature algorithms,

wherein said multi-signed public key certificate includes at least a basic area and an extended area, the basic area storing information identifying a first different signature algorithm executed by a first of the plurality of certificate authorities, and the extended area storing information identifying a second different signature algorithm executed by a second of the plurality of certificate authorities, and

wherein attaching digital signatures includes generating first and second signatures by respectively applying the first and second different signature algorithms to information in both the basic area and the extended area.

7. (Previously Presented) The public key certificate issuing method according to claim 6, wherein at least one of said plurality of certificate authorities executes a step of generating a signature for a signed public key certificate by applying a signature algorithm which is different from that attached to said signed public key certificate and attaching the generated signature to said signed public key certificate.

8. (Original) The public key certificate issuing method according to claim 6, wherein said plurality of certificate authorities include a Rivest-Shamir-Adleman certificate authority for executing signature generation processing based on a Rivest-Shamir-Adleman signature algorithm and an elliptic curve cryptography certificate authority for executing signature generation processing based on an elliptic curve cryptography signature algorithm, said Rivest-Shamir-Adleman certificate authority executes signature generation processing based on said Rivest-Shamir-Adleman signature algorithm, said elliptic curve cryptography certificate authority executes signature generation processing based on said elliptic curve cryptography signature algorithm, and said multi-signed public key certificate, including a signature based on said Rivest-Shamir-Adleman signature algorithm and a signature based on said elliptic curve cryptography signature algorithm, is issued.

9. (Original) The public key certificate issuing method according to claim 6, wherein at least one of said plurality of certificate authorities executes processing of storing a generated signature and signature information including signature algorithm information associated with said generated signature into an extended areas of said public key certificate.

10. (Previously Presented)The public key certificate issuing method according to claim 6, wherein at least one of said plurality of certificate authorities executes processing of storing a generated signature into an area other than the basic area and the extended area of said public key certificate and storing signature information including signature algorithm information associated with said generated signature into said extended area.

11. (Original) The public key certificate issuing method according to claim 6, wherein at least one of said plurality of certificate authorities executes processing of storing, into said public key certificate, flag information indicating whether at least two signatures are included in said public key certificate.

12. (Original) An information processing apparatus for executing verification of a public key certificate, having a configuration for selecting, from among a plurality of signature algorithms recorded in signature information stored in a basic area and an extended area of said public key certificate, a signature algorithm which can be verified by said information processing apparatus and executing signature verification on the basis of the selected signature algorithm.

13. (Canceled)

14. (Canceled)

15. (Canceled)

16. (Canceled)

17. (Currently Amended) A program storage medium for providing a computer program for executing public key certificate issuing processing for issuing a public key certificate of an entity which uses said public key certificate, said computer program comprising the steps of:

storing basic data in a basic area of the public key certificate;

storing extended data in an extended area of the public key certificate;

generating a first signature ~~based on the~~ by applying a first signature algorithm ~~derived from~~ to the stored basic data and extended data, the first signature algorithm being executable by a first of a plurality of certificate authorities that each execute a different signature algorithm;

attaching the first digital signature to the public key certificate;

generating, with the use of a second signature algorithm different from that of the first signature attached to said public key certificate, a second signature by applying the second signature algorithm to the stored basic data and extended data, the second signature algorithm being executable by a second of the plurality of certificate authorities; and

attaching said second signature to said public key certificate.